Self Assessment

Patient Identification

General Instructions for the SAFER Self Assessment Guides

The SAFER Guides are designed to help healthcare organizations conduct self-assessments to optimize the safety and safe use of electronic health records (EHRs) in the following areas.

- High Priority Practices
- Organizational Responsibilities
- Contingency Planning
- System Configuration
- System Interfaces
- Patient Identification
- Computerized Provider Order Entry with Decision Support
- Test Results Reporting and Follow-Up
- Clinician Communication

Each of the nine SAFER Guides begins with a Checklist of "recommended practices." The downloadable SAFER Guides provide fillable circles that can be used to indicate the extent to which each recommended practice has been implemented. Following the Checklist, a Practice Worksheet gives a rationale for and examples of how to implement each recommended practice, as well as likely sources of input into assessment of each practice, and fillable fields to record team members and follow-up action. In addition to the downloadable version, the content of each SAFER Guide, with interactive references and supporting materials, can also be viewed on ONC's website at www.healthit.gov/SAFERGuide.

The SAFER Guides are based on the best evidence available at this time (2013), including a literature review, expert opinion, and field testing at a wide range of healthcare organizations, from small ambulatory practices to large health systems. The recommended practices in the SAFER Guides are intended to be useful for all EHR users. However, every organization faces unique circumstances and will implement a particular practice differently. As a result, some of the specific examples in the SAFER Guides for recommended practices may not be applicable to every organization.

The SAFER Guides are designed in part to help deal with safety concerns created by the continuously changing landscape that healthcare organizations face. Therefore, changes in technology, clinical practice standards, regulations and policy, and associated industry practices should be taken into account when using the SAFER Guides. Periodic self-assessments using the SAFER Guides may also help organizations identify areas in which it is particularly important to address the implications of change for the safety and safe use of EHRs.

In some instances, Meaningful Use and/or HIPAA Security Rule requirements are identified in connection with recommended practices. The SAFER Guides are not intended to be used for legal compliance purposes, and implementation of a recommended practice does not guarantee compliance with Meaningful Use, HIPAA, or other laws. The SAFER Guides are for informational purposes only and are not intended to be an exhaustive or definitive source. They do not constitute legal advice or offer recommendations based on a healthcare provider's specific circumstances. Users of the SAFER Guides are encouraged to consult with their own legal counsel with regard to compliance with Meaningful Use, HIPAA, and other laws. For more information on Meaningful Use, please visit the Centers for Medicare & Medicaid Services website at www.cms.gov. For more information on HIPAA, please visit the HHS Office for Civil Rights website at www.hhs.gov/ocr.

Self Assessment

Patient Identification

Introduction

The *Patient Identification SAFER Guide* identifies recommended safety practices associated with the reliable identification of patients in the EHR. Accurate patient identification ensures that the information presented by and entered into the EHR is associated with the correct person. Processes related to patient identification are complex and require careful planning and attention to avoid errors. In the EHR-enabled healthcare environment, providers rely on technology to help support and manage these complex identification processes. Technology configurations alone cannot ensure accurate patient identification.[1] Staff also must be supported with adequate training and reliable procedures.

This self-assessment can help identify and evaluate where breakdowns related to patient identification occur in the healthcare setting. The self-assessment focuses on processes within organizations related to the creation of new patient records, patient registration, retrieval of information on previously registered patients, and other types of patient identification activities. The recommended practices can help prevent or detect and mitigate problems caused by duplicate records, patient mix-ups, and "comingled" (or "overlay") records.[2-11]

This guide is meant to support and enable patient matching technology and capabilities, focusing on best practices for improving data accuracy, which is the first necessary step to ensuring accurate patient matching. However, patient matching between organizations is not the focus of this guide. The recommended practices in this Patient Identification SAFER Guide provide support for many, varied patient matching technologies, as well as alternatives and best practices on specific patient attributes for patient matching, which are likely to change over time.

Completing the self-assessment in the *Patient Identification SAFER Guide* requires the engagement of people both within and outside the organization (such as EHR technology developers). Because this guide is designed to help organizations prioritize EHR-related safety concerns, clinician leadership in the organization should be engaged in assessing whether and how any particular recommended practice affects the organization's ability to deliver safe, high quality care. Collaboration between clinicians and staff members while completing the self-assessment in this guide will enable an accurate snapshot of the organization's patient identification status (in terms of safety), and even more importantly, should lead to a consensus about the organization's future path to optimize EHR-related safety and quality: setting priorities among the recommended practices not yet addressed, ensuring a plan is in place to maintain recommended practices already in place, dedicating the required resources to make necessary improvements, and working together to prevent and mitigate the highest priority patient identification-related safety risks introduced by the EHR.

Self Assessment

Patient Identification

Table of Contents

The SAFER Self Assessment Guides were developed by health IT safety researchers and informatics experts:

Joan Ash, *PhD MLS, MS, MBA, Professor and Vice Chair, Department of Medical Informatics and Clinical Epidemiology, School of Medicine, Oregon Health & Science University*;

Hardeep Singh, *MD, MPH, Associate Professor of Medicine at the Michael E. DeBakey Veterans Affairs Medical Center and Baylor College of Medicine and Chief of the Health Policy, Quality and Informatics Program at the Houston VA HSR&D Center of Excellence, and Director of the Houston VA Patient Safety Center of Inquiry; and*

Dean Sittig, *PhD, University of Texas School of Biomedical Informatics at Houston, UT-Memorial Hermann Center for Healthcare Quality & Safety.*

This guide was developed under the contract Unintended Consequences of Health IT and Health Information Exchange, Task Order HHSP23337003T/HHSP23320095655WC.

The *Checklist* is structured as a quick way to enter and print your self-assessment. Your selections on the checklist will automatically update the related section of the corresponding recommended practice worksheet.

The *Phase* associated with the *Recommended Practice(s)* appears at the top of the column. Click on the link to access more information about the Phases and Principles from the website.

The *Recommended Practice(s)* for the topic appear below the associated *Phase*.

Recommended Practices for ***Phase 1 — Safe Health IT***

			Implementation Status			
			Fully in all areas	Partially in some areas	Not implemented	
1	Hardware that runs applications critical to the organization's operation is duplicated.	Worksheet 1	○	○	○	reset
2	An electric generator and sufficient fuel are available to support the EHR during an extended power outage.	Worksheet 2	○	○	○	reset
3	Paper forms are available to replace key EHR functions during downtimes.	Worksheet 3	○	○	○	reset
4	Patient data and software application configurations critical to the organization's operations are backed up.	Worksheet 4	○	○	○	reset
5	Policies and procedures are in place to ensure accurate patient identification when preparing for, during, and after downtimes.	Worksheet 5	○	○	○	reset

Recommended Practices for ***Phase 2 — Using Health IT Safely***

			Implementation Status			
			Fully in all areas	Partially in some areas	Not implemented	
6	Staff are trained and tested on downtime and recovery procedures.	Worksheet 6	○	○	○	reset
7	A communication strategy that does not rely on the computing infrastructure exists for downtime and recovery periods.	Worksheet 7	○	○	○	reset
8	Written policies and procedures on EHR down-times and recovery processes ensure continuity of operations with regard to safe patient care and critical business operations.	Worksheet 8	○	○	○	reset
9	The user interface of the locally maintained backup, read-only EHR system is clearly differentiated from the live/production EHR system.	Worksheet 9	○	○	○	reset

Recommended Practices for ***Phase 3 — Monitoring Safety***

			Implementation Status			
			Fully in all areas	Partially in some areas	Not implemented	
10	There is a comprehensive testing and monitoring strategy in place to prevent and manage EHR down-time events.	Worksheet 10	○	○	○	reset

Select the level of *Implementation* achieved by your organization for each *Recommended Practice*.

Your *Implementation Status* will be reflected on the *Recommended Practice Worksheet* in this PDF.

To the right of each *Recommended Practice* is a link to the *Recommended Practice Worksheet* in this PDF.

The Worksheet provides guidance on implementing the Practice.

*Recommended Practices for **Phase 1 — Safe Health IT***

			Implementation Status			
			Fully in all areas	Partially in some areas	Not implemented	
1	An enterprise-wide master patient index that includes patients' demographic information and medical record number(s) from different parts of the same organization is used to identify patients before importing data.	*Worksheet 1*	○	○	○	reset
2	Clinicians can select patient records from electronically generated lists based on specific criteria (e.g., user, location, time, service).	*Worksheet 2*	○	○	○	reset
3	Information required to accurately identify the patient is clearly displayed on all computer screens, wristbands, and printouts.	*Worksheet 3*	○	○	○	reset
4	Patient names on adjacent lines in the EHR display are visually distinct.	*Worksheet 4*	○	○	○	reset
5	Medical record numbers incorporate a "check digit" to help prevent data entry errors.	*Worksheet 5*	○	○	○	reset
6	Users are warned when they attempt to create a new record for a patient (or look up a patient) whose first and last name are the same as another patient.	*Worksheet 6*	○	○	○	reset

*Recommended Practices for **Phase 2 — Using Health IT Safely***

			Implementation Status			
			Fully in all areas	Partially in some areas	Not implemented	
7	Patients are registered using a centralized, common database using standardized procedures.	*Worksheet 7*	○	○	○	reset
8	The user interfaces of the training, test, and read-only backup versions of the EHR are clearly different from the production ("live") version to prevent inadvertent entry or review of patient information in the wrong system.	*Worksheet 8*	○	○	○	reset
9	The organization has a process to assign a "temporary" unique patient ID (which is later merged into a permanent ID) in the event that either the patient registration system is unavailable or the patient is not able to provide the required information.	*Worksheet 9*	○	○	○	reset

*Recommended Practices for **Phase 2 — Using Health IT Safely***

			Implementation Status			
			Fully in all areas	Partially in some areas	Not implemented	
10	Patient identity is verified at key points or transitions in the care process (e.g., rooming patient, vital sign recording, order entry, medication administration, and check out).	*Worksheet 10*	○	○	○	reset
11	The EHR limits the number of patient records that can be displayed on the same computer at the same time to one, unless all subsequent patient records are opened as "Read Only" and are clearly differentiated to the user.	*Worksheet 11*	○	○	○	reset
12	Patients who are deceased are clearly identified as such.	*Worksheet 12*	○	○	○	reset
13	The use of test patients in the production (i.e., "live") environment is carefully monitored. When they do exist, they have unambiguously assigned "test" names (e.g., including numbers or multiple ZZ's) and are clearly identifiable as test patients (e.g., different background color for patient header).	*Worksheet 13*	○	○	○	reset

*Recommended Practices for **Phase 3 — Monitoring Safety***

			Implementation Status			
			Fully in all areas	Partially in some areas	Not implemented	
14	The organization regularly monitors their patient database for patient identification errors.	*Worksheet 14*	○	○	○	reset

A multidisciplinary team should complete this self-assessment and evaluate potential health IT-related patient safety risks addressed by this specific SAFER Guide within the context of your particular healthcare organization.

This Team Worksheet is intended to help organizations document the names and roles of the self-assessment team, as well as individual team members' activities. Typically team members will be drawn from a number of different areas within your organization, and in some instances, from external sources. The suggested Sources of Input section in each Recommended Practice Worksheet identifies the types of expertise or services to consider engaging. It may be particularly useful to engage specific clinician and other leaders with accountability for safety practices identified in this guide.

The Worksheet includes fillable boxes that allow you to document relevant information. The Assessment Team Leader box allows documentation of the person or persons responsible for ensuring that the self-assessment is completed. The section labeled Assessment Team Members enables you to record the names of individuals, departments, or other organizations that contributed to the self-assessment. The date that the self-assessment is completed can be recorded in the Assessment Completion Date section and can also serve as a reminder for periodic reassessments. The section labeled Assessment Team Notes is intended to be used, as needed, to record important considerations or conclusions arrived at through the assessment process. This section can also be used to track important factors such as pending software updates, vacant key leadership positions, resource needs, and challenges and barriers to completing the self-assessment or implementing the Recommended Practices in this SAFER Guide.

Assessment Team Leader

Assessment Completion Date

Assessment Team Members

Assessment Team Notes

reset page

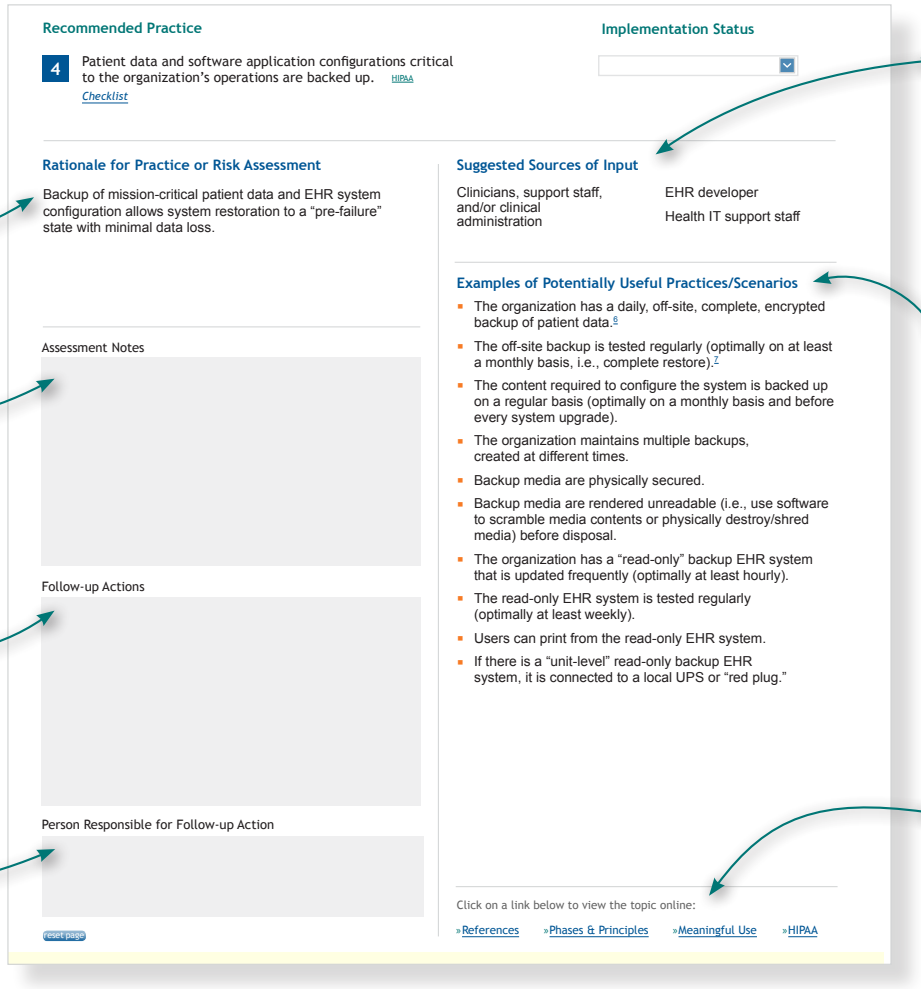
Each *Worksheet* provides guidance on implementing a specific *Recommended Practice*, and allows you to enter and print information about your self-assessment.

The *Rationale* section provides guidance about "why" the safety activities are needed.

Enter any notes about your self-assessment.

Enter any follow-up activities required.

Enter the name of the person responsible for the follow-up activities.



The *Suggested Sources of Input* section indicates categories of personnel who can provide information to help evaluate your level of implementation.

The *Examples* section lists potentially useful practices or scenarios to inform your assessment and implementation of the specific *Recommended Practice*.

Each *Worksheet* shows links to additional information available on the website.

Recommended Practice

1 An enterprise-wide master patient index that includes patients' demographic information and medical record number(s) from different parts of the same organization is used to identify patients before importing data.[12]

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Duplicate patient records are a common problem and can cause harm when clinicians lack complete records. Likewise, when two patients' records are commingled harm can result. An enterprise-wide master patient index reduces the occurrence of duplicate patient records by increasing the likelihood that patients with previous encounters are identified.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- The master patient index employs a probabilistic matching algorithm that uses patient's first and last names, date of birth, gender, and other attributes, such as zip code or telephone number or the last four digits of the social security number.[13]
- Organizations have policies and procedures to identify and prevent duplicate patient records and integrate unintentional duplicate records into one complete record.
- Organizational policies address how to ensure correct patient identification of information from external sources, such as external labs, pharmacies or healthcare providers, and how to monitor compliance with those policies.
- Organizations update policies on patient identification related to the master patient index as best practices change.

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

2 Clinicians can select patient records from electronically generated lists based on specific criteria (e.g., user, location, time, service).[14]

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Selecting a patient from a short list of relevant patients reduces the risk of selecting the wrong patient.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- Patient lists can be automatically generated in several formats to provide information relevant to a clinical or administrative need: person-specific (e.g., all patients that a clinician is responsible for), location-specific (e.g., all patients on a particular nursing unit or clinic), time-specific (e.g., all patients on today's schedule), and service-specific (e.g., all patients being cared for by a particular specialty or service).
- Clinicians can view (read), edit (write: create, modify, delete), and use (execute: select a patient) patient lists related to their own clinical purposes.
- Patient lists should by sorted in a clinically relevant order by default (e.g., by room number or appointment time), rather than alphabetically, to reduce the chance of look-alike or sound-alike names appearing close together.
- There are 2 or more patient identifiers included with each patient on the list (e.g., name & date of birth, Medical record number, gender).[15]

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

3 Information required to accurately identify the patient is clearly displayed on all computer screens, wristbands, and printouts.[16]

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Providing medical services to the wrong patient is one of the most common preventable sources of patient harm. Steps should be taken to ensure that the person using an EHR to care for a patient is addressing the intended patient. Doing so reduces the risk of wrong patient errors.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- Organizational policies and all computer-generated displays incorporate the following information to facilitate patient identification, with appropriate exceptions for individuals (e.g., victims of domestic violence) for whom such information could create other risks:
  - Last name, first name, date of birth (with calculated age)
  - Gender
  - Medical record number
  - In-patient location (or home address or ZIP code)
  - Recent photograph (recommended)
  - Responsible physician (optional)
- Organizational policies and workflows incorporate use of the EHR into ensuring correct patient identification.

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

4 Patient names on adjacent lines in the EHR display are visually distinct.
Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Keeping patient names visually distinct in the EHR reduces the likelihood of unintentionally selecting the wrong patient. This is a basic good usability practice.

Suggested Sources of Input

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- On all patient lists containing two or more patients with the same last name, the names in common are displayed in a visually distinct manner (e.g., bold, italics, different color).
- Use alternate line colors for adjacent patients.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

5 Medical record numbers incorporate a "check digit" to help prevent data entry errors.

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

A "check digit" program for reducing common errors in number sequences used in patient records greatly reduces data entry errors.[17]

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- Organizational policies optimize automated processes in the EHR to prevent common errors, including transposition errors, which can result in poor patient identification.
- One example of a "check digit" program is the "Verhoeff algorithm," which works with strings of decimal digits of any length and detects all single-digit errors and all transposition errors involving two adjacent digits.[18]

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

6 Users are warned when they attempt to create a new record for a patient (or look up a patient) whose first and last name are the same as another patient.

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Using automated EHR processes to prevent duplicate records can prevent unintentional human errors that could lead to patient harm. Creating a duplicate (split) record or commingling two different patient records results in a serious patient safety risk.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- System generates an alert when a user attempts to create a record for a new patient or looks up an existing patient with the same first and last name as an existing patient.
- System generates an alert when a user attempts to create a record for a new patient or looks up an existing patient with a similar sounding first and last name as an existing patient, using a phonetic algorithm such as Soundex.
- System monitors for similar names (nicknames), or changed last names (e.g., marriage, divorce, adoption), when other demographics match.
- Alert provides additional demographic information context for the existing patient to help the user confirm or rule out that it is the same patient.

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

7 Patients are registered using a centralized, common database using standardized procedures.

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Nonstandard registration practices and lack of access to a common database are common causes of duplicate medical records on the same patient.

Suggested Sources of Input

Clinicians, support staff, and/or clinical administration

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- Organizational policy establishes standardized registration procedures involving the EHR and a common database to serve as the "source of truth" on whether a record already exists on a person who presents for services.
- The organization requires a picture ID[19] when verifying the identity of new patients (with appropriate alternatives for minors and others who do not have official picture IDs).
- The organization uses a picture ID (or appropriate alternative when an official picture ID is not available) or uses biometric attributes (e.g., iris or vein scan) to authenticate the identity of established patients.
- Registration clerks are trained to look up patients using the enterprise master patient index before creating a new record.
- When new patient records are being created during the registration process, the registrar is prompted to consider other potential matches in the existing database.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

8 The user interfaces of the training, test, and read-only backup versions of the EHR are clearly different from the production ("live") version to prevent inadvertent entry or review of patient information in the wrong system. HIPAA

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

If a clinician logs into and begins using the training, test, or read-only backup versions of the EHR by mistake, any information he or she attempts to enter will be lost.

Suggested Sources of Input

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- The screen background color on the production ("live") EHR is different from all other EHR environments.
- EHR users are trained to understand the meaning of the visual differences between the different environments.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

9 The organization has a process to assign a "temporary" unique patient ID (which is later merged into a permanent ID) in the event that either the patient registration system is unavailable or the patient is not able to provide the required information.[20] HIPAA

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Inevitably, in certain cases, care must be delivered to patients who are not yet registered. Processes must be in place to ensure that they soon have a permanent ID and to merge records to avoid duplicate or incomplete records.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- A process (automated or manual, such as naming conventions) is in place to assign temporary IDs to newborns and patients arriving at the Emergency Department unable to provide their demographic information.
- Staff members are trained in areas where temporary IDs may be required to ensure that temporary records are integrated into permanent ones.
- Any downstream use of a temporary ID, such as in billing or in transfers between facilities, is tracked and corrected in all electronic systems, including at transfer facilities.
- Organizations monitor resolution of temporary IDs.

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

10 Patient identity is verified at key points or transitions in the care process (e.g., rooming patient, vital sign recording, order entry, medication administration, and check out).

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

To avoid wrong patient errors, care must be taken to check the patient's identification at all critical points in the healthcare process and to ensure that EHR use is integrated into workflows that support correct patient identification.

Suggested Sources of Input

Clinicians, support staff, and/or clinical administration

Examples of Potentially Useful Practices/Scenarios

- Before opening a specific patient record or signing an order, the user is shown a picture, or the name, gender, and age of the patient.[21]
- Clinicians are asked to "re-enter" the patient's initials before signing an order.
- Workflow related to verification of patient identity is evaluated to optimize use of the EHR to prevent wrong patient errors.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

11 The EHR limits the number of patient records that can be displayed on the same computer at the same time to one,[22] unless all subsequent patient records are opened as "Read Only" and are clearly differentiated to the user. HIPAA

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Distractions while documenting or reviewing information in the EHR are common. EHRs should be designed to reduce the likelihood of working with the wrong patient's record as the result of distractions. When working on multiple patients, potential gains in efficiency are outweighed by the risks associated with entering or reviewing data on the wrong patient.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Suggested Sources of Input

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- Clinicians are engaged in developing EHR configuration and policies to prevent errors due to distractions and the resulting danger of working on the wrong patient chart when more than one is open.
- Workflow is evaluated to ensure that clinicians are able to respond to urgent situations in which they may need to look at a new record without completing review of a first patient. The practice environment should be designed to minimize the need to open and actively use more than one patient's records on the same computer.
- Before allowing the user to change the current patient, the system checks that all entered data has been saved (i.e., signed) before allowing the system to display a different patient's data.[23]

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

12 Patients who are deceased are clearly identified as such.
Checklist

Implementation Status

Rationale for Practice or Risk Assessment

In many instances selection of a deceased patient represents a "wrong patient" error. Clinicians should be reminded that the patient they have selected is dead.

Suggested Sources of Input

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- The system displays either a pop-up alert when opening the record or a different background color for the deceased patient header in the EHR.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

13 The use of test patients in the production (i.e., "live") environment is carefully monitored. When they do exist, they have unambiguously assigned "test" names (e.g., including numbers or multiple ZZ's) and are clearly identifiable as test patients (e.g., different background color for patient header). HIPAA

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Test patients in the production system are necessary to facilitate end-to-end testing, but care must be taken to ensure that they are not mistaken for "real" patients.

Suggested Sources of Input

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- Test patients should have names that clearly identify them as such: BWH17, ZZZOrders or MGH23zz, ZResults (examples are Last, First).
- "Cute" names, e.g., "Marcus Welby" or "Jim Test" should not be used as test patients since there could be real patients with those names.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA

Recommended Practice

14 The organization regularly monitors their patient database for patient identification errors.[11,24] HIPAA

Checklist

Implementation Status

Rationale for Practice or Risk Assessment

Avoidable patient identification errors are a risk both to patients and to the organizations. Monitoring reduces the likelihood that patients will be misidentified and harmed as a result.

Suggested Sources of Input

EHR developer

Health IT support staff

Examples of Potentially Useful Practices/Scenarios

- Organizations have a policy to periodically monitor their EHR database for common scenarios related to wrong patient identification.
- The order–retract–reorder algorithm can be used to estimate the rate of erroneous orders due to patient ID errors.[21]
- The "inconsistent gender algorithm" can be used to estimate the number of erroneous freetext notes due to patient ID errors.[24]
- Once identified through monitoring, duplicate records are detected and merged.
- Industry standards for duplicate record error rates are available. The organization consistently monitors its own duplicate record error rate, and ensures that it remains at or below industry standards.

Assessment Notes

Follow-up Actions

Person Responsible for Follow-up Action

reset page

Click on a link below to view the topic online:

»References »Phases & Principles »HIPAA